FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare si Tehnologia Informatiei
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	7.

2. Date despre disciplină

2.1 Denumirea disciplinei				***Auditul sistemelor informatice și managementul riscurilor de securitate***	
2.2 Titularii de curs				Dr. ing. Dan LUȚAȘ (dlutas@bitdefender.com)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				Ing. Nicolae Bodea - nicubodea96@gmail.com	
2.4 Anul de studiu	I	2.5 Semestrul	2	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	3	din care:	Curs	2	Seminar	1	Laborator		Proiect	
3.2 Număr de ore pe semestru	42	din care:	Curs	28	Seminar	14	Laborator		Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										48
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										18
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										15
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	83
3.5 Total ore pe semestru (3.2+3.4)	125
3.6 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Securitatea informațiilor
4.2 de competenţe	Arhitecturi de calculatoare, Sisteme de operare

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Tabla, proiector, calculatoare
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Tabla, proiector, calculatoare

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	C1. Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatice • C1.1 – Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice avansate aferente domeniului general al securității informațiilor și sistemelor de calcul. Cunoașterea conceptelor aferente riscurilor, evaluării riscurilor și managementului securității • C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de

	securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou • C1.3 – Modelarea unor noi tipuri de riscuri de securitate, evidențierea impactului asupra utilizatorului, asupra sistemelor și aplicațiilor existente. Identificarea unor soluții posibile și evaluarea lor • C1.4 – Stabilirea limitelor maxime de securitate oferite de soluții nou propuse. Plasarea corectă a riscurilor de securitate și a posibilelor soluții într-un cadru de repere bine cunoscute anterior • C1.5 – Elaborarea de modele teoretice noi de analiză a proprietăților de securitate sau evaluarea securității oferite de diverse soluții C3. Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • C3.1 – Cunoașterea teoretică și practică a diverselor scenarii de configurare sau mentenanță greșită a sistemelor de calcul, precum și a claselor de vulnerabilități software și atacuri informatice tipice • C3.2 – Analiza și înțelegerea unor protocoale de comunicare și module software noi, pentru identificarea unor vulnerabilități posibile. Utilizarea listelor dedicate, recunoscute în domeniu, de clase și tipuri de vulnerabilități și configurări greșite pentru analiza și validarea unui sistem informatic nou din punct de vedere al securității • C3.3 – Capacitatea de a analiza critic, din punctul de vedere al testării vulnerabilității, configurarea unei rețele, sistem de calcul sau aplicații software, fără să existe informații anterioare. Capacitatea de a identifica informații vizibile, servicii expuse etc. • C3.4 – Evaluarea limitărilor teoretice și practice oferite de diverse metode și tehnologii de detectare a vulnerabilităților și configurărilor greșite ale sistemelor de calcul. Determinarea unor corelări constructive între diverse metode de detecție
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Familiarizarea studenților cu noțiunile și elementele de bază ale activităților de audit și management de securitate a sistemelor informaționale și conferirea capacității de a înțelege procesul de audit al sistemelor informaționale, conform standardelor internaționale (ISACA)
7.2 Obiectivele specifice	1. Înțelegerea procesului de auditare a sistemelor informaționale, cu referire la standardele internaționale (ISACA) 2. Înțelegerea procesului de guvernare și management IT, împreună cu activitatea de audit al guvernării și managementului IT 3. Înțelegerea proceselor de achiziție, dezvoltare și implementare a sistemelor informaționale, împreună cu activitatea de audit al acestor procese 4. Înțelegerea proceselor de operare, întreținere și suport a sistemelor informaționale, asigurarea continuității afacerii și planurilor de recuperare în caz de dezastru, împreună cu activitatea de audit al acestor procese 5. Înțelegerea procesului de asigurare a protecției sistemelor informaționale (managementul securității sistemelor informaționale, controlul accesului, securitatea infrastructurii de rețea, securitatea fizică), împreună cu activitatea de audit aferentă

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Introducere în managementul securității și auditul sistemelor Informatice	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Guvernarea IT (roluri și responsabilități, strategii de securitate, politici, standarde și proceduri, metrici de guvernare)	2		
Auditul guvernării IT	2		

Managementul riscului (evaluarea riscului - evaluarea vulnerabilităților, evaluarea amenințărilor, analiză, monitorizare) și auditul managementului riscului	2		
Planificarea continuității afacerii și recuperarea după dezastru (audit și administrare - analiza Impactului, RPO/RTI, copii de siguranță)	2		
Tratarea incidentelor (proceduri de răspuns la incidente, dezvoltarea unui plan de răspuns la incidente, testarea răspunsului la incidente/BCP/DRP)	2		
Managementul proiectelor software: ciclul de viață a dezvoltării software, fazele de certificare și acreditare, sisteme de aplicații business (comerț electronic, schimbul electronic de date, aplicații bancare, transfer electronic de fonduri)	2		
Auditul managementului de proiect	2		
Operațiuni de securitate informațională (administrarea patch-urilor, administrarea configurațiilor) și întreținere, audit (sisteme de operare, infrastructură de rețea)	2		
Administrarea securității informaționale (framework-uri, audit), acces logic (controlul accesului software, identificare, autorizare), acces fizic și audit	2		
Securitatea infrastructurii de rețea (LAN, WAN, Wireless, Firewall, IDS, IPS, VoIP, PBX, testarea vulnerabilităților de rețea)	2		
Auditul infrastructurii de rețea (a componentelor prezentate în cursul 11)	2		
Managementul securității informației (guvernare, managementul riscului, dezvoltarea și gestionarea unui program de securitate a informației)	2		
Prezentare de sinteză a subiectelor studiate, evidențierea concluziilor esențiale, discuții si prezentări pe subiecte propuse de studenți	2		

Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)*

1. CISA Certified Information Systems Auditor Study Guide (Cannon, David – 2011 – Sybex) (3rd ed)
2. IT Auditing Using Controls to Protect Information Assets (Davis, Chris – 2011 – McGraw-Hill) (2nd ed)
3. CISM Review Manual 2013 (ISACA – 2012 – ISACA) (11th edition)
4. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (Landoll, Douglas – 2011 – CRC Press) (2nd ed)
5. Diferite articole

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Importanța securității & auditului sistemelor informatice	1	Expuneri la tablă, explicații suplimentare, discuții	
Management-ul riscului. Recuperarea după dezastru: tehnici și principii	1		
Importanța patch-urilor de securitate. Securitate de rețea	1		
Analiza unor rapoarte tehnice și articole recente: vulnerabilități în sistemele de operare	1		
Analiza unor rapoarte tehnice și articole recente: vulnerabilități în infrastructura de rețea	1		
Analiza unor rapoarte tehnice și articole recente: vulnerabilități în aplicații	1		
Analiza unor rapoarte tehnice și articole recente: atacuri avansate	1		

Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziția studenților într-un număr de exemplare corespunzător)*

1. CISA Certified Information Systems Auditor Study Guide (Cannon, David – 2011 – Sybex) (3rd ed)
2. IT Auditing Using Controls to Protect Information Assets (Davis, Chris – 2011 – McGraw-Hill) (2nd ed)
3. CISM Review Manual 2013 (ISACA – 2012 – ISACA) (11th edition)

4. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (Landoll, Douglas – 2011 – CRC Press) (2nd ed)
5. Diferite articole

*Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.
Cursuri de audit și security risk management sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- IT&C Audit – IT&C Security Master Program - THE BUCHAREST ACADEMY OF ECONOMIC STUDIES, http://ism.ase.ro/files/Curriculum/Y2012-2014/analytical-programs/en/S4/ISM_PA_EN_024.pdf
- Information Technology Auditing - Master of Science in Information Systems Audit and Control – Georgia State University, http://cis.robinson.gsu.edu/academic-programs/ms-is-audit/curriculum/
- Audit & Security - Information Security and Audit, MSc – University of Greenwich http://www2.gre.ac.uk/study/courses/pg/inftec/isa/cms-courses?banner=COMP1431&cyear=1415

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs	Examen scris și/sau de tip grilă pe platforma Moodle. In situații excepționale, care necesită desfășurarea activităților didactice de la distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	60%
Seminar	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de seminar	Prezentarea unei teme de cercetare din domeniul cursului și/sau rezolvarea și prezentarea soluției unor probleme similare cu cele discutate în timpul orelor de seminar. In situații excepționale, care necesită desfășurarea activităților didactice de la distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	40%
Laborator	-	-	-
Proiect	-	-	-

Standard minim de performanţă
Curs. Prezența la **minim 50%** din orele de curs, pentru admiterea la examenul final.
Aplicații. Prezența la seminar **obligatorie 100%** (un seminar se poate recupera în timpul semestrului, iar altul în sesiunile de restanțe) pentru admiterea la examenul final.
Capacitatea de a defini și explica în context noțiunile de bază a activităților de audit al sistemelor informaționale și management al securității sistemelor informaționale, cum ar fi: procesul de audit, procesul de guvernare și management IT, procesele de achiziție, dezvoltare, implementare, operare, întreținere, suport și asigurare a protecției sistemelor informaționale, împreună cu mecanismele de audit specifice fiecărui proces.

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
	Curs	Dr. ing. Dan LUȚAȘ	
	Aplicații	Ing. Nicolae Bodea	

Data avizării în Consiliul Departamentului Calculatoare	Director Departament Prof.dr.ing. Rodica Potolea
Data aprobării în Consiliul Facultății de Automatică și Calculatoare	Decan Prof.dr.ing. Liviu Miclea